REMARKS

Claims 1-7, 9-16, 18-27, 29-44, 46 and 47 are pending in the present application. This Amendment is in response to the Office Action mailed February 25, 2009. In the Office Action, the Examiner rejected claims 1-7, 9, 11-15, 17-25, 30, 31, 39-44, and 46-47 under 35 U.S.C. §103(a). Applicant respectfully submits that claims 23, 28, 32-38 and 45 have been previously cancelled. Applicant has amended claim 1 and has added claim 48. Applicant submits that the newly-added claims introduce no new substantive matter. Reconsideration in light of the remarks made herein is respectfully requested.

Request for an Examiner's Interview

Applicant respectfully requests the Examiner to contact the undersigned attorney if, after his review, there are still questions regarding patentability. Such discussions will greatly facilitate the prosecution of this case. The undersigned attorney can be reached at the telephone number listed below.

Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 1-7, 9, 11-15, 17-25, 30, 31, 39-44, and 46-47 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 6,938,164 issued to England et al. (England '164) in view of Bruce Schneier's "Applied Cryptography, Second Edition" (Schneier), and further in view of U.S. Patent No. 7,036,023 issued to Fries ("Fries"). Furthermore, claim 10 was rejected under 35 U.S.C. §103(a) as being unpatentable over England '164 in view of Tetrault's "ATPM – Review: Virtual PC 4.0 (Tetrault) and claims 16, 26, and 27 were rejected under 35 U.S.C. §103(a) as being unpatentable over England '164 in view of U.S. Patent No. 6,330,670 (England '670). Applicant respectfully traverses the rejection and submits that the Examiner has not met the burden of establishing a *prima facie* case of obviousness.

To establish a *prima facie* case of obviousness, certain basic criteria must be met. For instance, the prior art reference (or references when combined) must teach or suggest all the claim limitations. *See MPEP §2143.* Applicant respectfully submits that none of the cited references, most notably England '164, describes or suggests the limitations alleged in the Office Action.

Furthermore, the Supreme Court in *Graham v. John Deere*, 383 U.S. 1, 148 USPQ 459 (1966), stated: "Under §103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined." *See MPEP 2141.* In *KSR International Co. vs. Teleflex, Inc.*, 127 S.Ct. 1727 (2007) (Kennedy, J.), the Court explained that "[o]ften, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order *to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.*" *Emphasis Added.* The Court further required that an explicit analysis for this reason must be made. "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *KSR 127 S.Ct.* at 1741, quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006). In the instant case, Applicant respectfully submits that there are significant differences between the cited references and the claimed invention and there is no apparent reason to combine the known elements in the manner as claimed, and thus no *prima facie* case of obviousness has been established.

The Examiner alleges that England '164 teaches "performing a start secure operation by a first processor of a plurality of processors" and "performing a join secure operation by remaining processors of the plurality of processors excluding the first processor, the join secure operation performed from the start secure operation", as recited in claim 1, citing column 4, lines 43-54. Applicant respectfully disagrees and submits that England '164, column 4, lines 43-54, merely states:

> "After computer 100 has been powered-on, one of CPUs 102, 104 will eventually begin executing instructions. Only one of CPUs 102, 104 may initially begin executing instructions, or alternatively one of CPUs 102, 104 may be selected to begin booting the computer. Any of a wide variety of arbitration mechanisms can be used to determine which of multiple CPUs is to begin booting the computer, such as a pre-configured default processor, a distributed arbitration

> scheme, an arbitration device or component (not shown) coupled to processor bus 112, etc." (England '164, col. 4, lines 44-53).

Accordingly, the Examiner alleges that one of the CPUs 102,104 beginning to execute instructions corresponds to "performing a start secure operation by a first processor of a plurality of processors" and that determining which of the multiple CPUs is to begin booting the computer corresponds to "performing a join secure operation by remaining processors of the plurality of processors excluding the first processor." Applicant respectfully disagrees.

As provided in England '164, the determination of which of the CPUs is to begin booting is either performed by assigning a default processor to boot the computer, by using a distributed arbitration scheme or an arbitration device (England '164, col. 4, lines 44-53). The determination itself is not performed by the remaining processors, as alleged by the Examiner.

Additionally, the Examiner alleges that England '164 discloses "the join secure operation performed automatically from the start secure operation" (Office Action, page 3). *Emphasis Added.* Applicant respectfully submits that dependent claim 48 recites "the join secure operation is performed atomically from the start secure operation". *Emphasis Added.* In England '164, there is no teaching that the determination of which CPU is to boot the computer, allegedly the join secure operation, is performed atomically, as set forth in claim 48.

Further, England '164 discloses initialization of trusted core 146 beginning in response to a "Trusted Core Initialization" command issued by one of CPUs 102, 104 during booting of computer 100 (England '164, col. 9, lines 34-37). *Emphasis Added.* Upon receipt of the Trusted Core Initialization command, the memory controller 106 protects memory 110 from all CPUs 102, 104 (England '164, col. 10, lines 12-14). The memory controller 106 prevents CPUs 102, 104 from issuing read or write requests, thereby preventing CPUs 102, 104 from accessing memory 110 (England '164, col. 10, lines 55-59).

While the Examiner previously alleged that the determination of which CPU is to boot the computer corresponds to the "join secure operation", the Examiner now alleges that the protection of the memory 110 upon receipt of "Trusted Core Initialization" command

corresponds to the "join secure operation" (Office Action, page 4). Applicant respectfully disagrees.

As stated in England '164, the CPUs performing the booting of the computer 100, allegedly the first processor, issues the Trusted Core Initialization, and the memory controller 106 prevents the CPUs 102,104, allegedly the first processor and the remaining processors, from issuing read or write requests.

Thus, since the memory controller 106, rather than the "remaining processors", is performing the protection of the memory 110 upon receipt of Trusted Core Initialization command, allegedly the "join secure operation", England '164 fails to teach "performing a join secure operation by remaining processors of the plurality of processors excluding the first processor", as recited in the claim.

Further, the CPUs being prevented from issuing read or write requests cannot correspond to "a halted state" given that the CPUs 102, 104 are allegedly the first processor and the remaining processors, and both CPUs 102, 104 being prevented from issuing read or write requests (England '164, col. 10, lines 55-59). In contrast, claim 1 states "a halted state that prevents the remaining processors from interfering with the operations of the first processor", claims 12 and 21 state "halting all but one of a plurality of processors in a computer", and claim 39 states "halting all processors of the plurality of processors except for the first processor from accessing the memory". Since the CPUs 102, 104, including the first processor and the remaining processors, are all prevented from issuing read or write requests, in England '164, all the processors are "halted" according to the Examiner's interpretation (England '164, col. 10, lines 55-59). Thus, England '164 fails to teach these elements of independent claims 1, 12, and 21.

In addition, England '164 merely discloses that the CPU, selected to boot the computer, begins loading and executing instructions. Eventually, a trusted core is loaded into memory 110 (England '164, col. 5, line 5-21). The memory controller 106 operates to ensure that trusted core, once loaded into memory 110, can be initialized (England '164, col. 9, lines 1-3). Upon receipt of the Trusted Core Initialization command, the memory controller 106 protects memory

110 from all CPUs 102, 104 (England '164, col. 10, lines 12-14). *Emphasis Added.* In contrast, the claims delineates "loading a content into the identified region under control by the first processor after receiving the signals that the remaining processors have entered the halted state" (claim 1), "loading content into the region only after the halting of all but the one of the plurality of processors" (claim 21), and "loading data into the selected area after the first processor receiving signaling from the at least one processor to indicate that the at least one processor is in a halted state" (claim 39). *Emphasis Added.*

Applicant respectfully submits that the loading of content, allegedly the trusted core, occurs prior to the memory controller 106 preventing the CPUs from issuing read or write requests, allegedly the halted state. As delineated in England '164, the memory controller 106 only prevents the CPUs from issuing read or write requests upon receipt of the trusted core initialization command (England '164, col. 10, lines 12-14) which occurs only once the trusted core is loaded into memory 110 (England '164, col. 9, lines 1-3). *Emphasis Added.* Thus, England '164 fails to teach these elements of the claims.

Moreover, the Examiner states that "although England '164 does not teach wherein signals are received by the first processor from the remaining processors that the remaining processors have been halted, and loading a content after this signal is received, this would have been obvious... England '164, as taught throughout the reference, only allows the system to operate when one CPU is active, and the others are in a halted state" (Office Action, page 5).

Applicant respectfully disagrees and submits that, as discussed above, England '164 fails to teach "a halted state" or "halting all but one of a plurality of processors" as delineated in claims 1, 12, 21, and 39 such that England '164 cannot in turn teach "receiving signals by the first processor from the remaining processors that the remaining processors have entered the halted state" (claim 1), "block access to the identified region by all resources except the non-halted CPU only after receiving signals by the one of the plurality of CPUs that a remainder of the plurality of CPUs have entered into a halted state" (claim 12), "loading content into the region only after the halting of all but the one of the plurality of processors" (claim 21), and

"loading data into the selected area after the first processor receiving signaling from the at least one processor to indicate that the at least one processor is in a halted state" (claim 39).

Therefore, Applicant respectfully requests the Examiner to withdraw the outstanding §103 rejection as applied to claims 1, 12, 21 and 39 as well as those claims dependent thereon.

Furthermore, claim 10 under 35 U.S.C. §103(a) as being unpatentable over England '164 combination as applied above, and further in view of ATPM – Review: Virtual PC 4.0 (April 2001), by Gregory Tetrault ("Tetrault"); and claims 16, 26, and 27 under 35 U.S.C. §103(a) as being unpatentable over England '164 combination as applied above, and further in view of U.S. Patent No. 6,330,670 issued to England et al. ("England"). Applicant respectfully traverses the rejection and submits that the Examiner has not met the burden of establishing a *prima facie* case of obviousness. However, given that these claims are dependent on claims which are considered by Applicant to be in condition for allowance, no discussion regarding the allowability of these claims is necessary.

Withdrawal of the outstanding §103(a) rejections as applied to claims 10, 16 and 26-27 is respectfully requested.

Conclusion

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: May 18, 2009

By /William W. Schaal/
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

1279 Oakmead Parkway
Sunnyvale, California 94085-4040